ISACA®

Bizalom és értékteremtés az információs rendszerekkel

Budapest Chapter

Információbiztonsági helyzetkép - 2012

Rónaszéki Péter, CISA, CISM, ISO27001LA
peter.ronaszeki@isaca.hu

A kutatásról

Jelen kutatásunk elsődlegesen az ISACA által képviselt négy szakmai területre fókuszál: IT audit, IT biztonság, IT irányítás, IT kockázatkezelés. A kutatás célcsoportját Magyarország azon „vezető" vállalatai és intézményei jelentették, amelyek a felmérés szempontjából relevánsnak tekinthetők, azaz vélelmezhető, hogy rendelkeznek a kérdések megválaszolásához szükséges IT biztonság/audit kompetenciákkal, és egyúttal a magyar gazdaság információbiztonság szempontjából leginkább releváns résztvevői.

A kutatás alapsokaságát a Listák Könyve alapján, ágazati besorolás szerint az egyes ágazatok legnagyobb cégei/intézményeinek leválogatásával állítottuk össze, kiegészítve a rendelkezésünkre álló nyilvános cégadatbázisok árbevétel szerint legnagyobb vállalatainak listájával. A teljes alapsokaság így mintegy 600 céget és intézményt tartalmaz, amelyek a fenti ismérvek szerint az ország információbiztonsági szempontból legjelentősebb gazdálkodó szervezeteinek tekinthetők.

Az így meghatározott sokaságból összesen 150 cég és intézmény töltötte ki a kérdőívet, amelyet online felületen keresztül tettünk elérhetővé számukra. A kérdőív kitöltői minden cég esetében az adott szervezet informatikai, információbiztonsági vezetői voltak, akik a szervezeten belül a leginkább kompetensnek tekinthetők a kérdőívben szereplő kérdések megválaszolása szempontjából.

A minta összetétele a főbb cégdemográfiai jellemzők szerint a következőképpen alakul.

	2011 [n=114]	2012 [n=150]
Működési terület	**%**	**%**
Költségvetési szféra		

minden cég esetében az adott szervezet [illegible] voltak, akik a szervezeten belül a leginkább kompetensnek tekinthetők a kérdőívben szereplő kérdések megválaszolása szempontjából.

A minta összetétele a főbb cégdemográfiai jellemzők szerint a következőképpen alakul.

	2011 [n=114]	2012 [n=150]
	%	%
Működési terület		
Költségvetési szféra	24	25
Magánszféra	76	75
Alkalmazotti létszám		
Kevesebb, mint 99 fő	10	19
100-499 fő	40	49
500 vagy több fő	50	31
Fő tevékenység		
Ipar	36	29
Távközlés, IT	13	13
Pénzügy	13	7
Oktatás, EÜ, költségvetési int.	24	26
Egyéb	14	26
Külföldi résztulajdon		
Nincs	50	54
Van	50	39
NT/NV	-	7

IT Audit: kettős kép – csökkenő gyakoriság, növekvő fontosság

Az IT audit elhagyása nem ritka probléma, a tavalyi évhez képest emelkedett azon cégek aránya, akik sem belső, sem külső auditot nem végeznek. Az audit fontossága tehát, úgy látszik, háttérbe szorul – holott ezzel gyakran komoly kockázatot vállalnak magukra azok a cégek, amelyek az IT audit költségeit próbálják ily módon csökkenteni vagy akár teljes egészében megspórolni. Ugyanakkor azok a szervezetek, amelyeknél megtartották [vagy bevezették] az audit funkciót, ennek egyre inkább felismerik a fontosságát, és ennek megfelelően pozícionálják a vállalaton belül.

Az audit egyre több vállalatnál kerül ki a vállalati IT irányítása alól

Általános – és Magyarországon is érvényes – trend, hogy ezt a feladatot kivonják az IT feladatköréből, hiszen ez – különböző személyi összefonódások, érdekviszonyok következtében – kihatással lehetne az audit eredményére is. Az IT Audit funkció leggyakrabban [és időben növekvő arányban] a nemzetközi ajánlásoknak megfelelően a vállalat felsővezetése/igazgatótanácsa felé tartozik beszámolással. A költségvetési szektorban ugyanakkor kevésbé érvényesül ez a pozitív tendencia, helyette itt az audit továbbra is az IT felé számol be.

Az auditorok személye és képzettsége egyre fontosabbá válik

Az auditot végző vagy végeztető vállalatok körében egyre koncentráltabban jelenik meg az az elvárás, hogy az auditot végző személyek CISA minősítéssel rendelkezzenek, amely garantálja a vállalatok számára, hogy az auditor megfelelő szakmai ismeretekkel, skillekkel és gyakorlattal rendelkezik – amely pedig elengedhetetlen ahhoz, hogy a vállalat teljes rálátást nyújtson valakinek üzletkritikus informatikai és biztonsági rendszereire. A CISA minősítés megkövetelése egyre jobban kiszorítja az egyéb megközelítéseket.

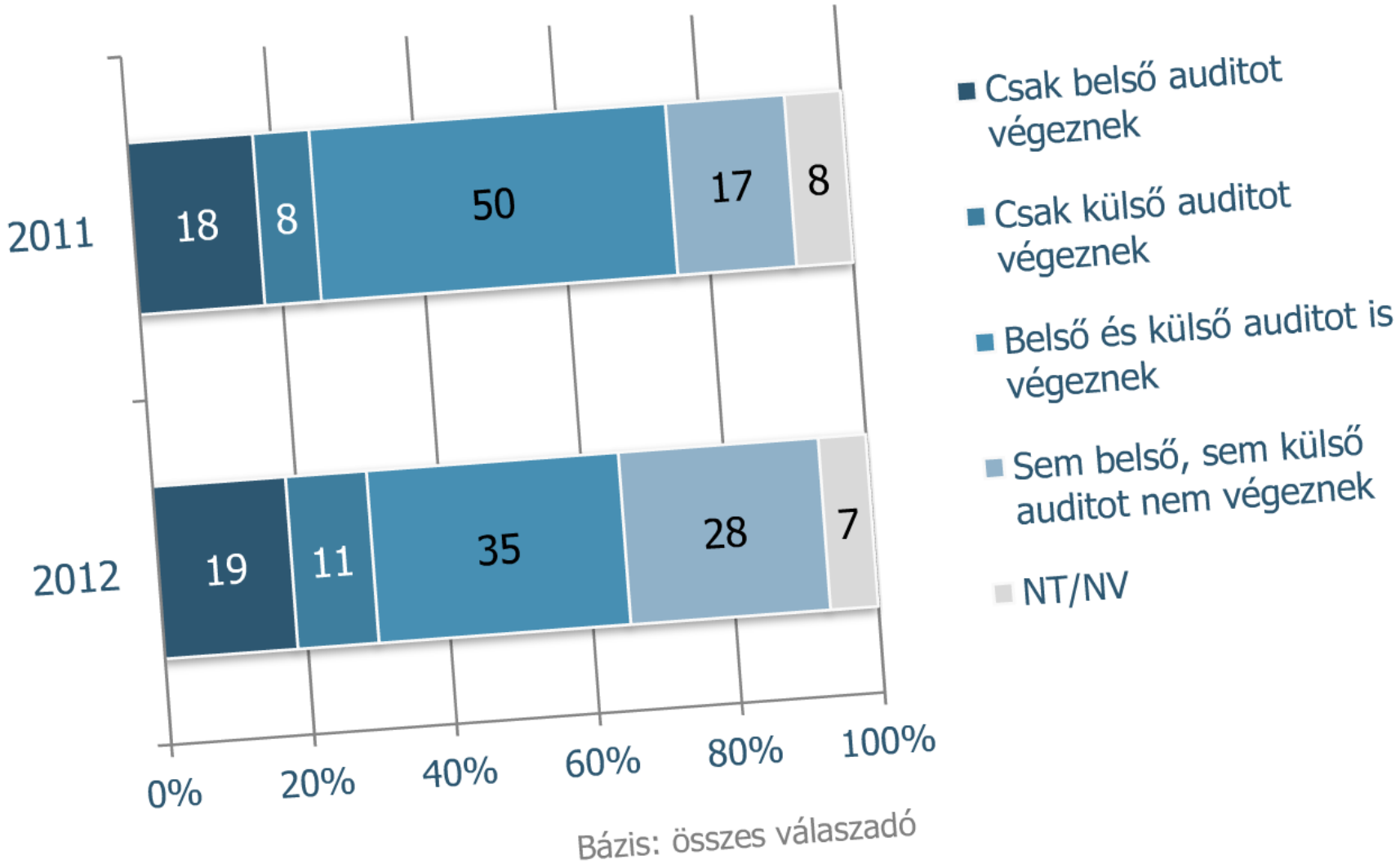
Az auditok fontosságának felismerését jelzi, hogy azok a vállalatok, ahol van audit, ezt egyre komolyabban is veszik: az átlagot meghaladó arányban végeznek teljesítményértékelést az auditorok munkájára vonatkozóan, és hajlamosak lennének akár többet is fizetni olyan auditért, amelyet kifejezetten az auditra vonatkozó minőségbiztosítási szabályok alapján végeznének.

Az információbiztonság stratégiai fontosságát már részben felismerték a magyar vállalatok, de az ennek érdekében tett konkrét lépések terén még távol vagyunk az élvonaltól

A magyarországi nagyvállalatok és a költségvetési intézmények körében is megfigyelhető jelenség, hogy az adminisztratív eszközök [biztonsági stratégiák, elhárítási tervek] használata dominál a technológiai védelmi/megelőző eszközök használatával szemben. Átfogó információbiztonsági stratégiája például a vállalatok/intézmények közel 50 százalékának van [egy nemzetközi összefoglaló tanulmány szerint ez világszerte átlagosan 65%], míg például sérülékenységelemző eszközökkel csak 14%-uk rendelkezik, szemben a nemzetközi szinten átlagosan 46%-os aránnyal.

kockázatok [illegible]
potenciális súlyossága tekintetében jelentősen csökkentve
és rendszerességgel elvégzett IT audit segítségével.

1. ábra: Végeznek-e rendszeresen [belső és/vagy külső] IT auditot a szervezetnél? [2011-2012]

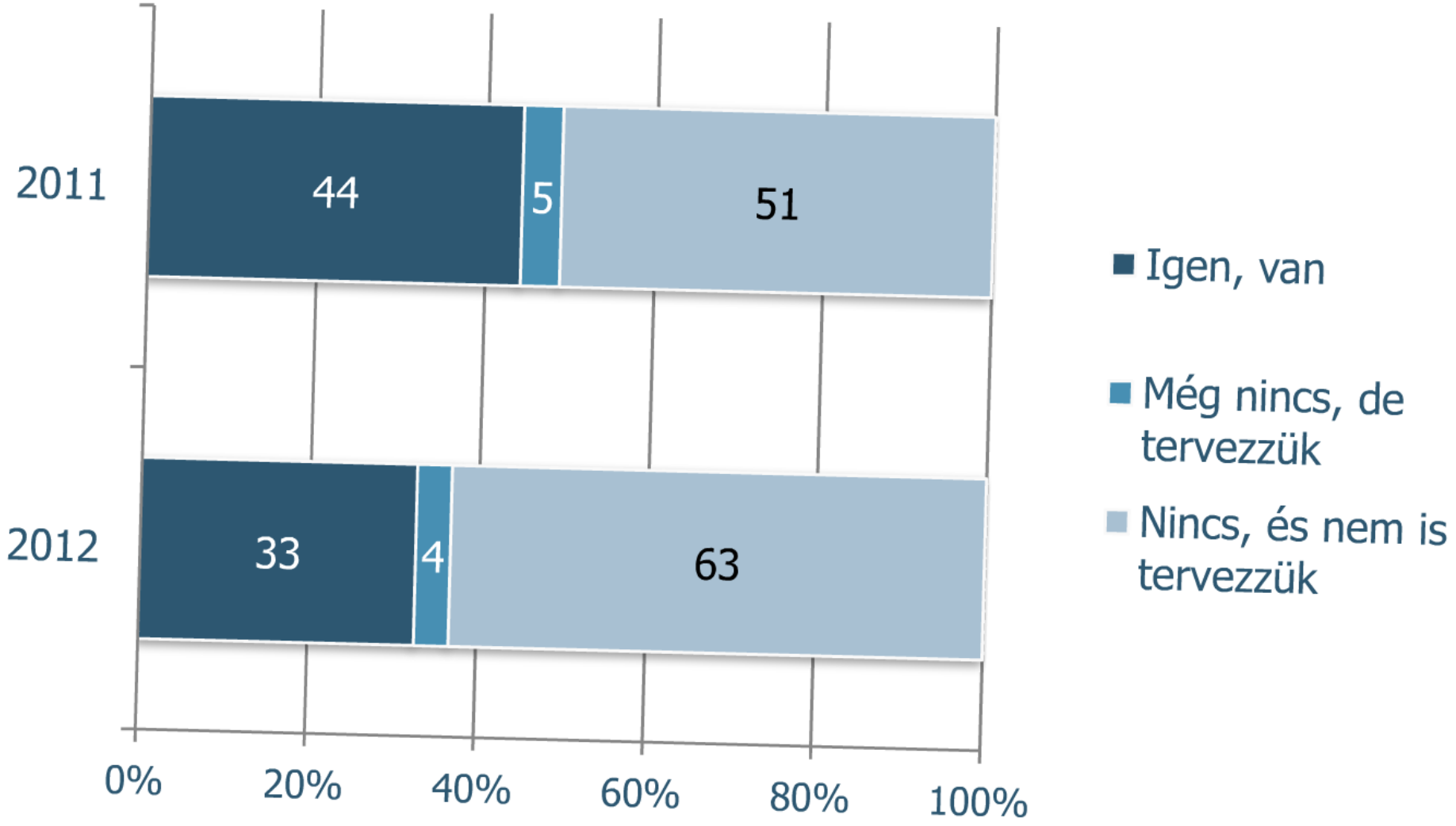


Bázis: összes válaszadó

A legjelentősebb hazai nagyvállalatok közel ötöde csak belső IT auditot végez és igen [illegible] auditot szervező cégek aránya is. Mindez komoly biztonsági [illegible] nézőpont kimaradása a

43%-os a belső és külső megoldász is alkalmazók aránya.

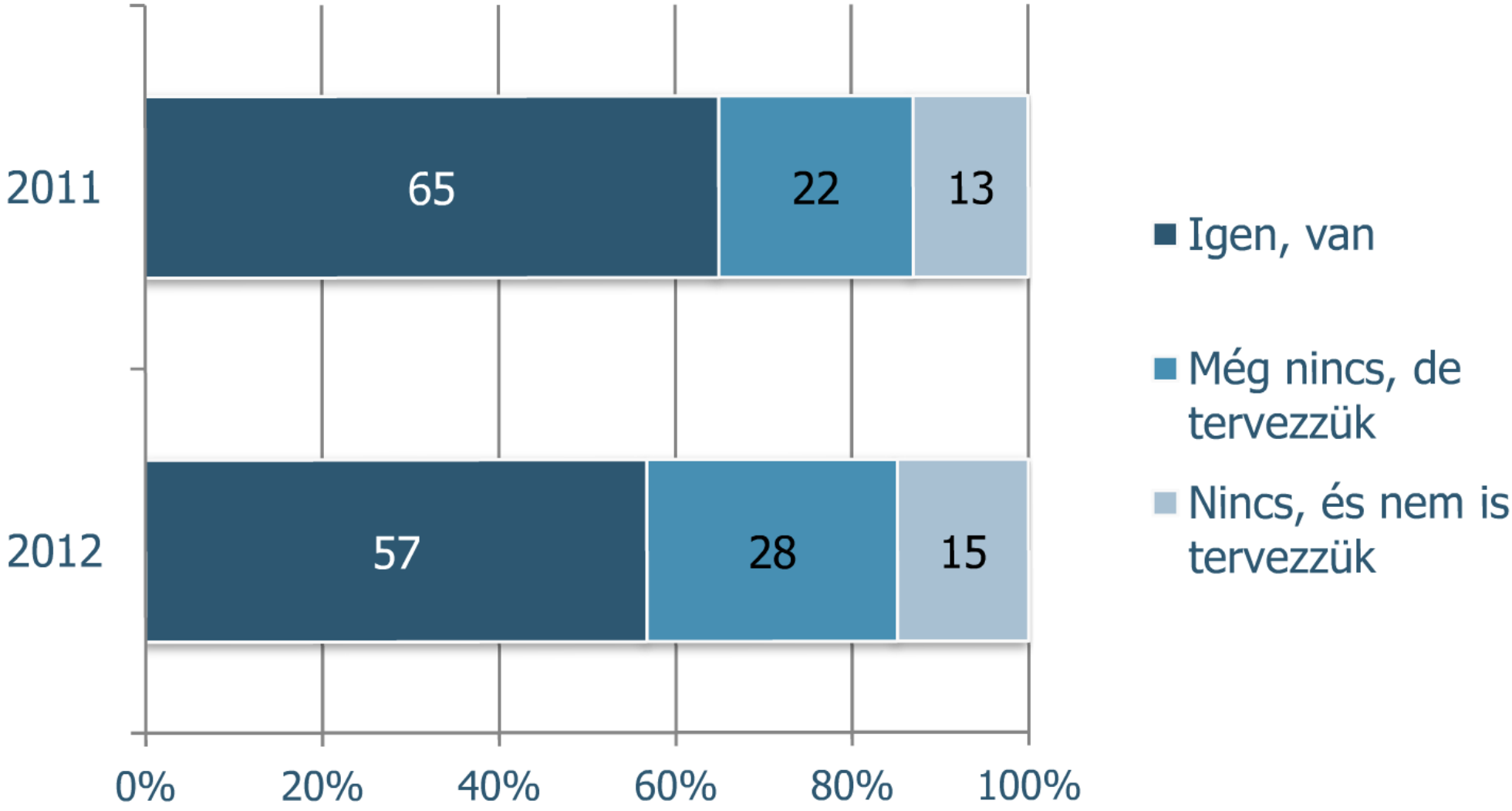
2. ábra: Van-e kiszervezés az IT audit területen? [2011-2012]



Bázis: IT auditot rendszeresen végző válaszadók

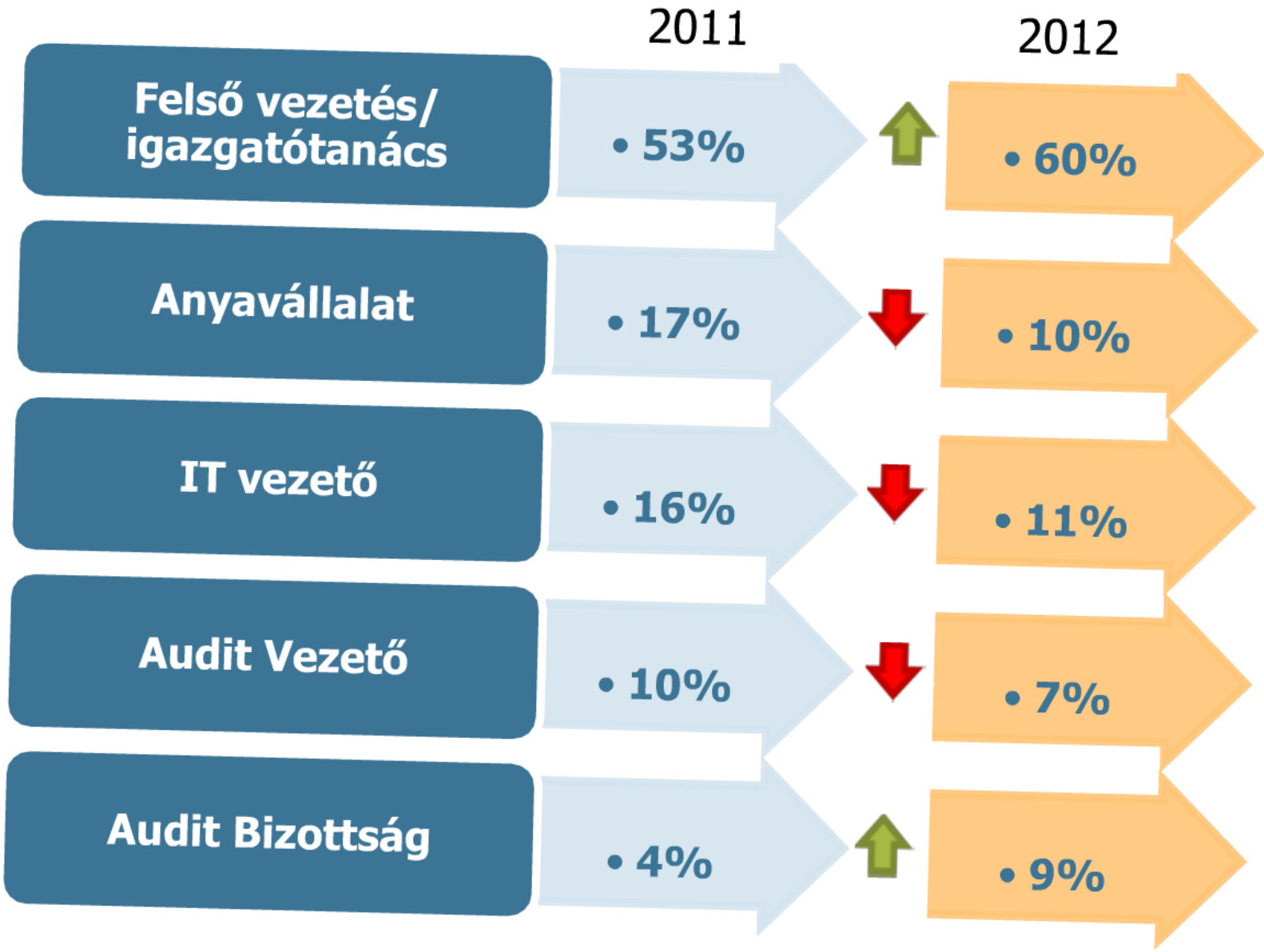
A vállalkozások életének legkülönbözőbb területein tapasztalható, hogy a core

3. ábra: Van-e részletes IT audit terv a szervezetnél? [2011-2012]



Bázis: belső IT auditot végző válaszadók

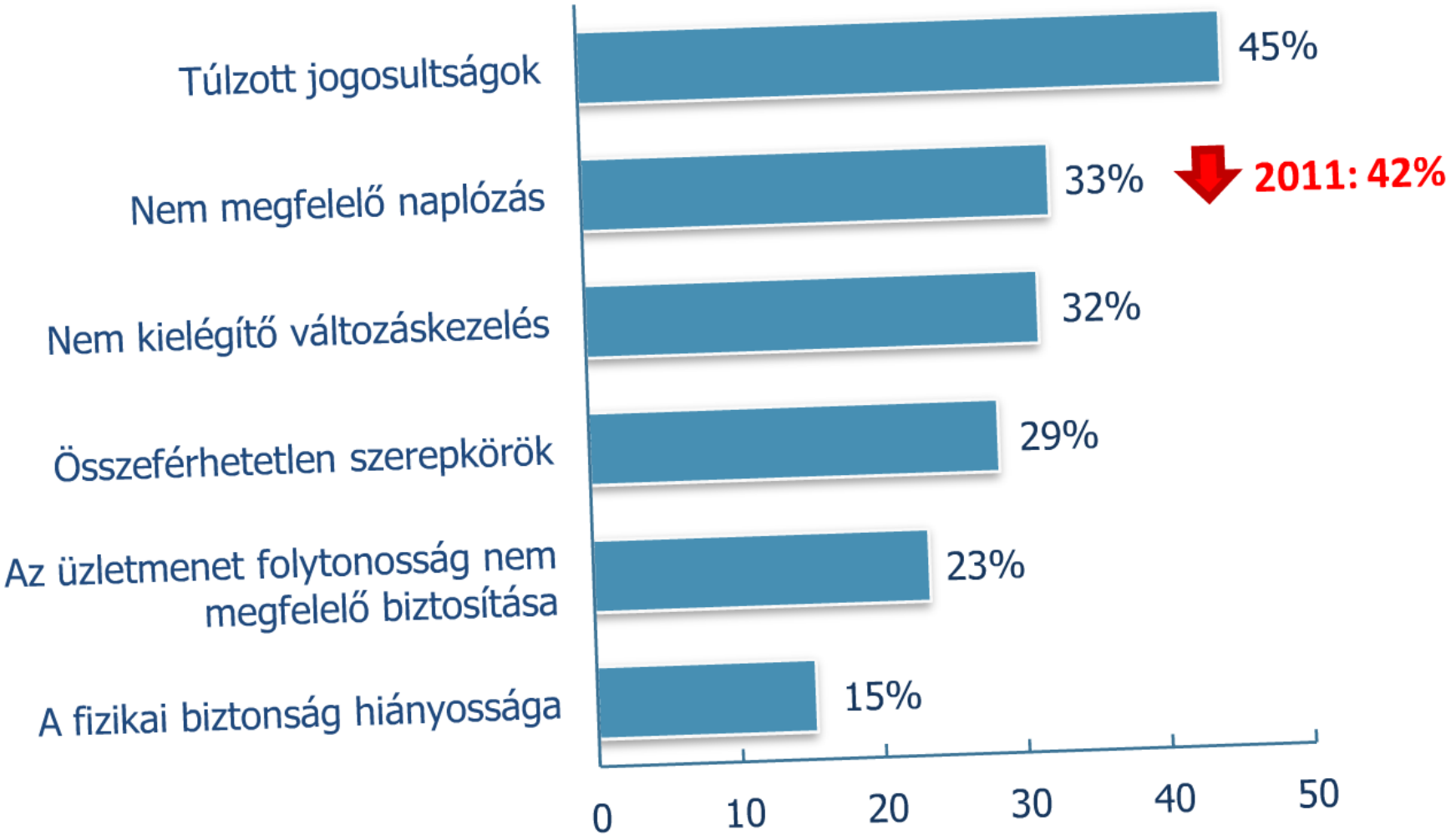
5. ábra: **Mely szervezeti egységnek tartozik beszámolással az IT audit funkció? [2011-2012]**



Bázis: belső IT auditot végző válaszadók

nemzetközi ajánlásoknak] megfeleloen probaljak is azt szamon
auditorokon, mind az auditált szervezeti egységeken.

6. ábra: Az IT auditok során azonosítottak-e hiányosságokat az alábbi területeken az elmúlt 12 hónapban? [2012]

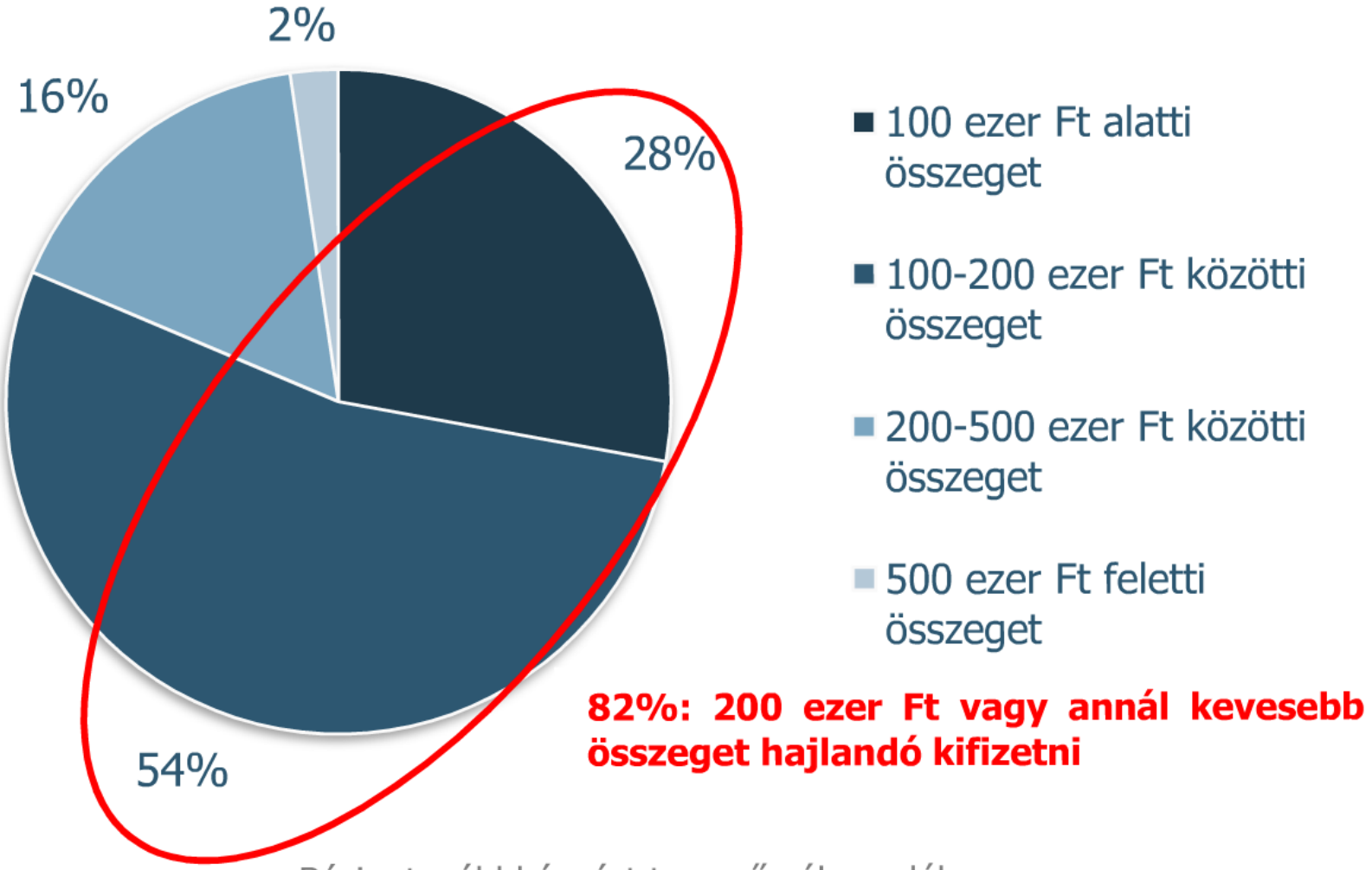


Bázis: IT auditot rendszeresen végző válaszadók

A vállalati IT auditok különböző biztonsági hiányosságot tárhatnak fel. Magyarországon

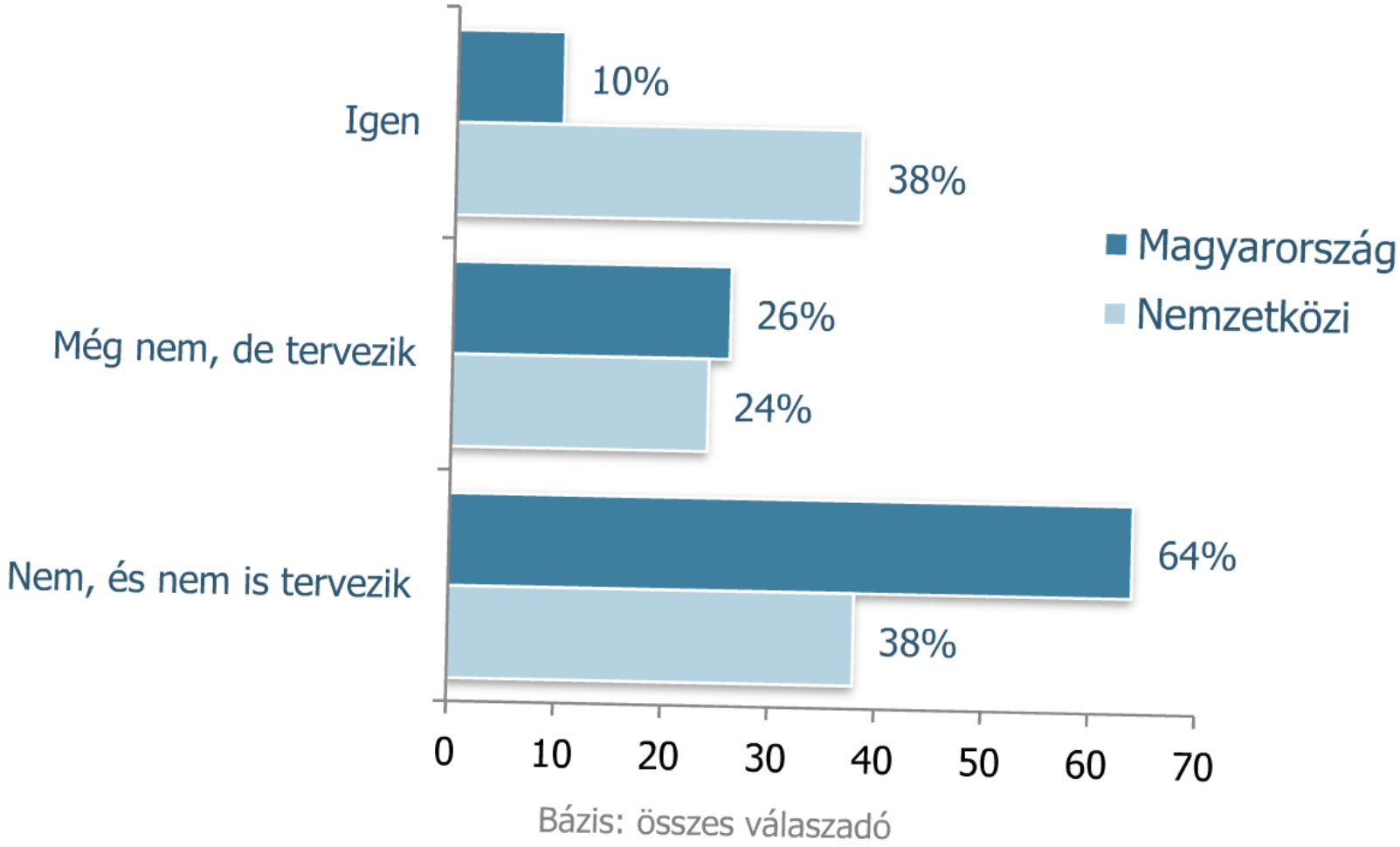
pedig negyedük kíván elkölteni egy évben egy munkatársa vonatkozóan.

15. ábra: Milyen forrást szánnak egy informatikai auditor továbbképzésére évente? [2012]



Bázis: továbbképzést tervező válaszadók

22. ábra: **Alakítottak-e már ki mérőszámrendszert az információbiztonsági terület működésének hatékonyságának vizsgálatára? [2012]**

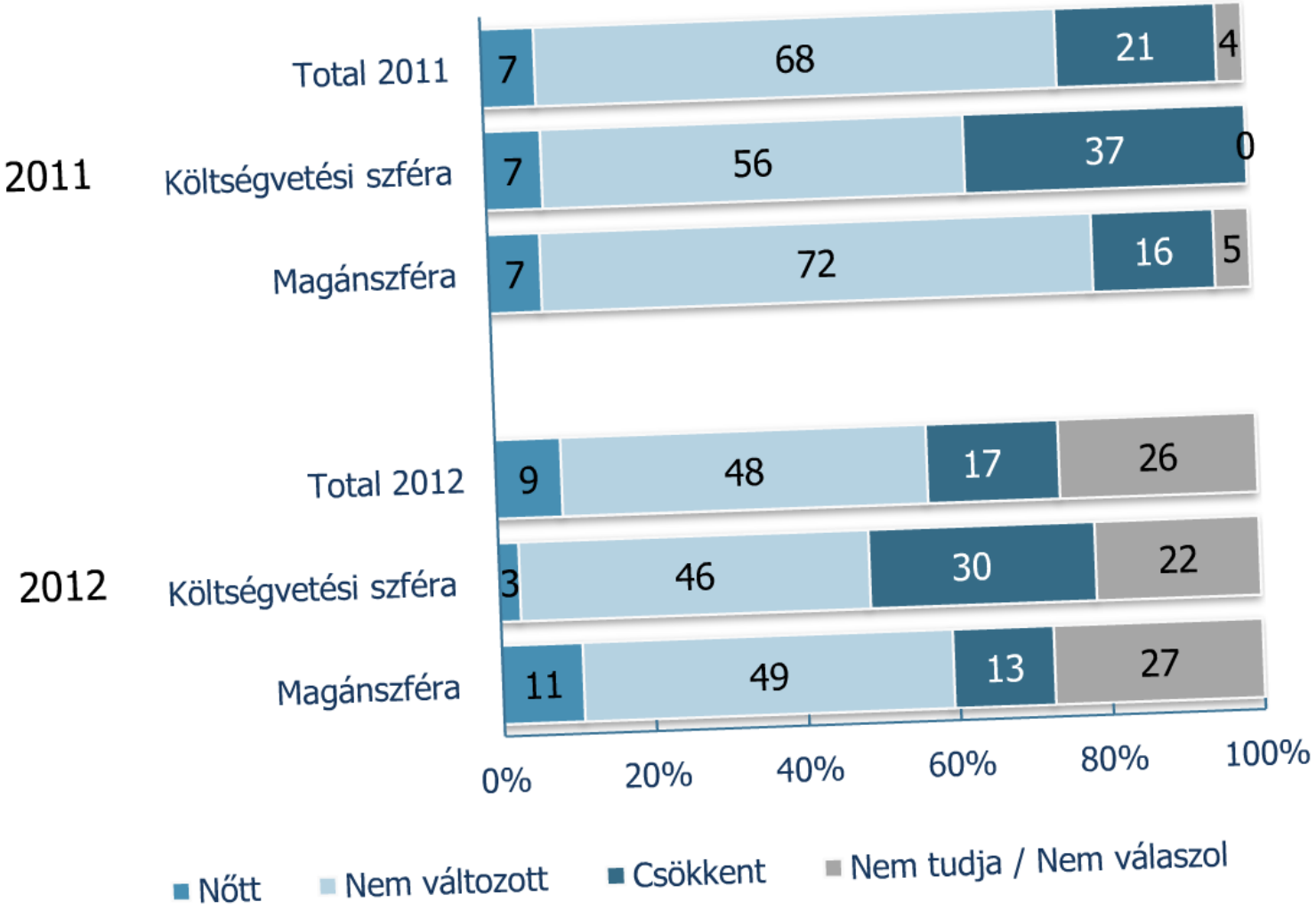


Bázis: összes válaszadó

A magyar gazdaság egészéhez képest valamivel kedvezőbb képet mutatnak a pénzügyi szektor vállalkozásai: 30% használ, 50% tervezi az információbiztonság hatékonyságát valamilyen standard metrikával vizsgálni. Ellenben a bűnügyi

rosszabb a helyzet, az intézmények 30 százaléka biztonsággal kapcsolatos kiadásait. A költségcsökkentés mértéke az érintett vállalatok és intézmények közel felénél a 20%-ot is meghaladta.

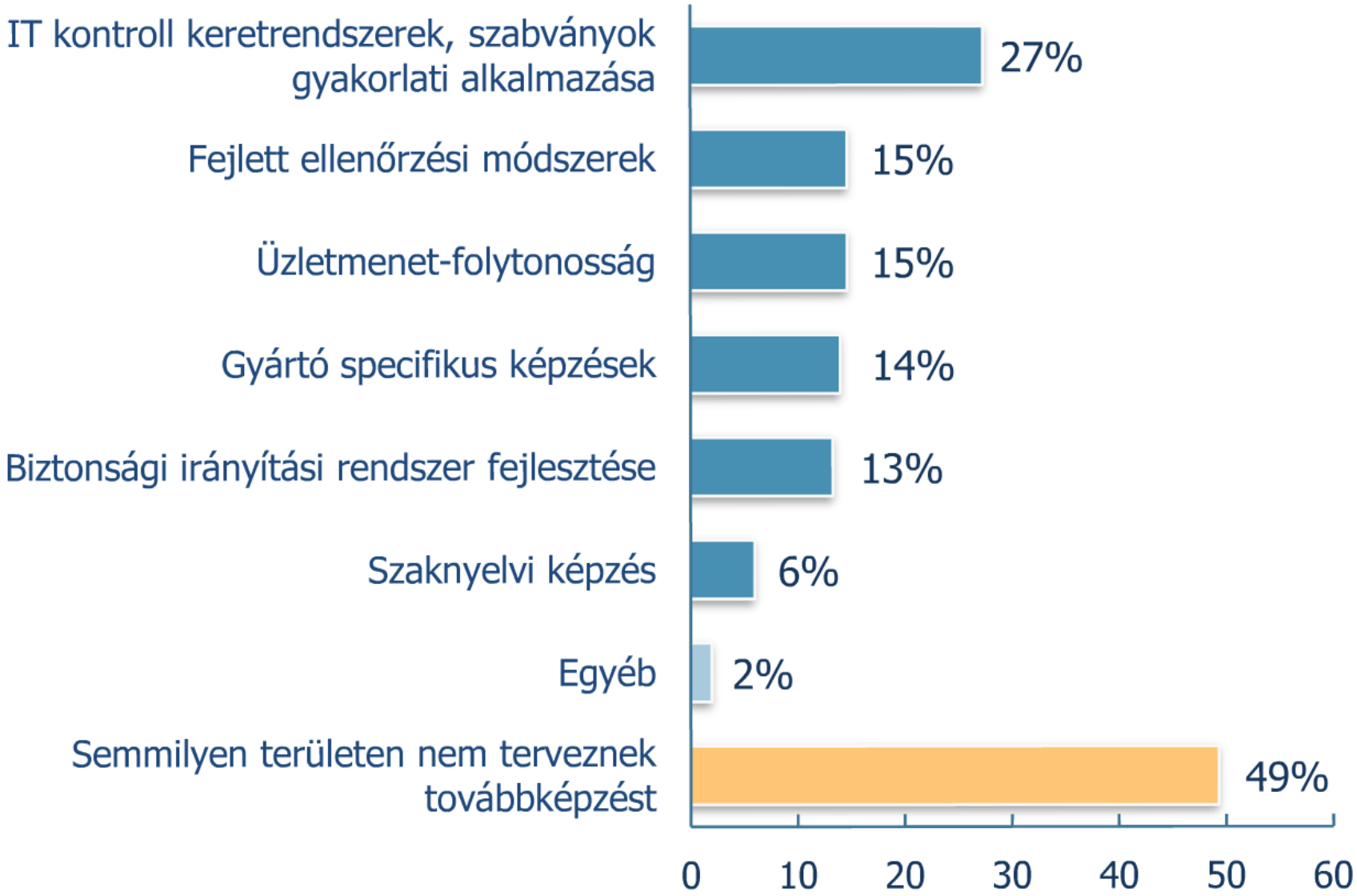
24. ábra: 2011-ben, ill. 2012-ben hogyan változott az információbiztonsági terület költségvetése az előző évhez [2010-hez/2011-hez] képest? [2011-2012]



Bázis: összes válaszadó

Biztonsági szakemberek képzettsége

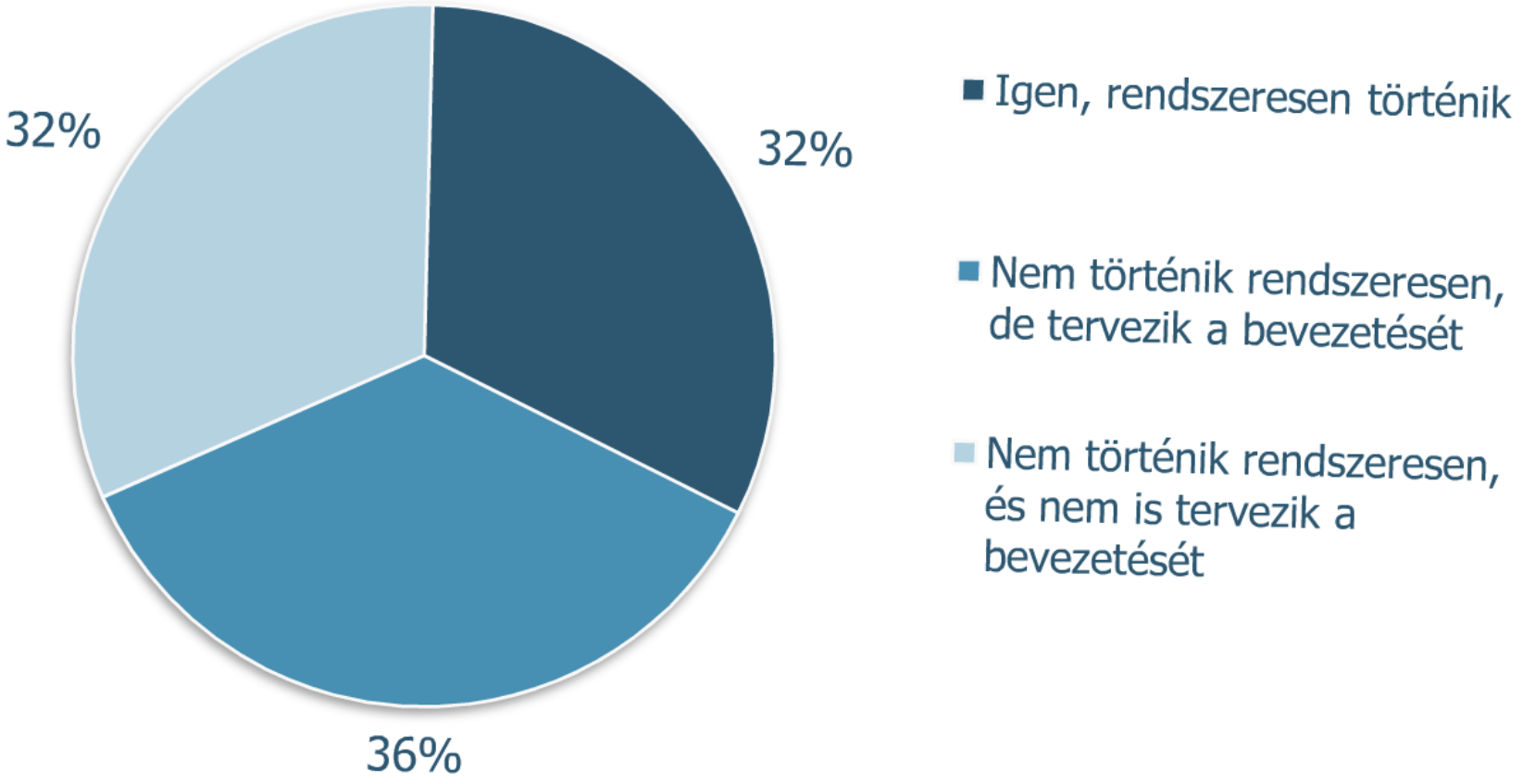
25. ábra: Milyen területen tervezik informatikai biztonsági szakembereiket továbbképezni? [2012]



Bázis: összes válaszadó

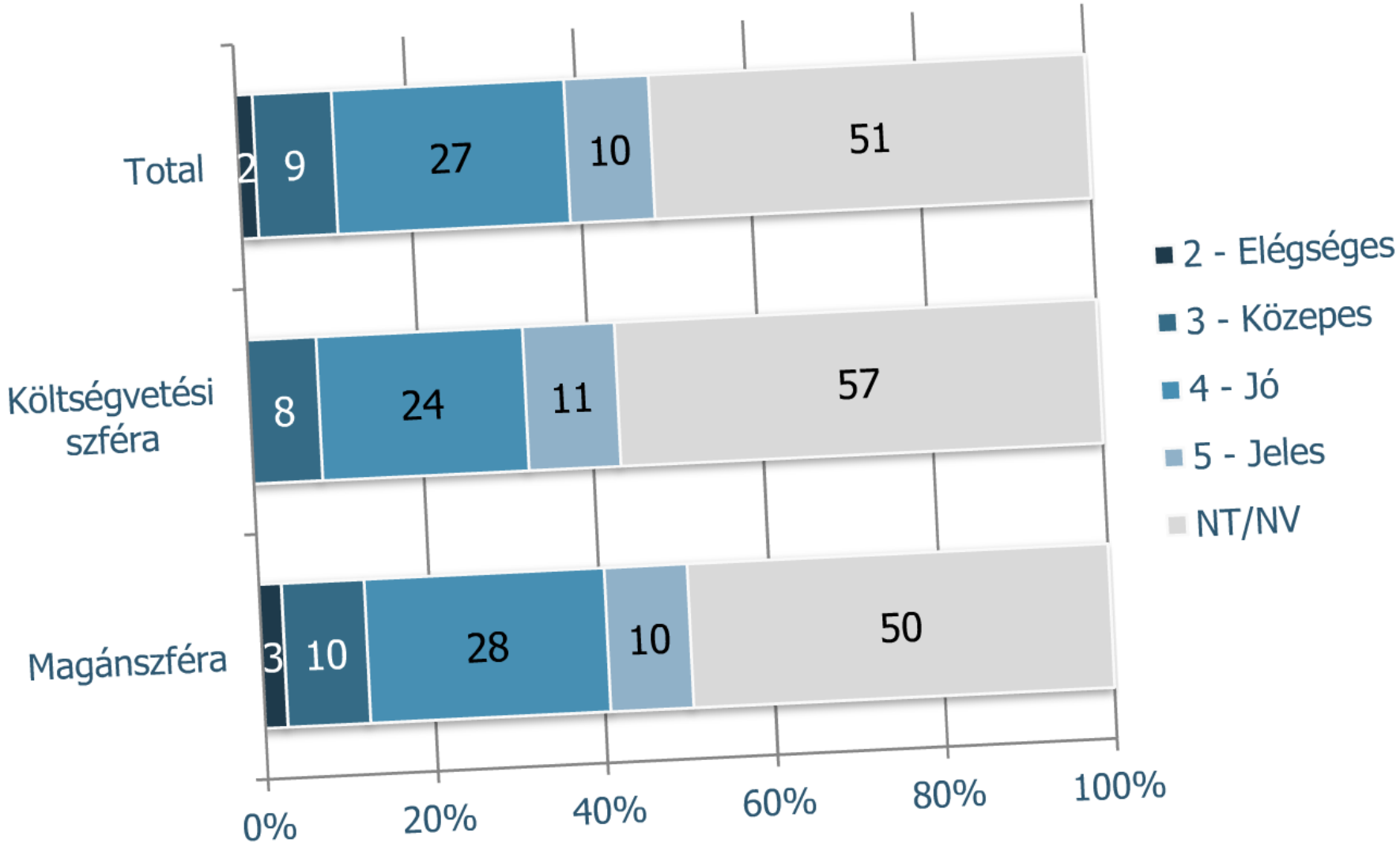
pénzügyi szektor jár ebben is az élen, ahol a vállalatok döntő többségénél már bevett szokás a rendszeres kockázatfelmérés.

30. ábra: Történik-e rendszeresen megfelelő mélységű IT kockázatfelmérés, illetve tervezik-e ennek bevezetését? [2012]



Bázis: összes válaszadó

32. ábra: Hogyan értékeli az ISACA Magyarországi Egyesület munkáját az elmúlt egy éveben? [Skálás kérdés, 1=elégtelen, 5=Jeles], **[2012]**



Bázis: összes válaszadó

ISACA®

Bizalom és értékteremtés az információs rendszerekkel

Budapest Chapter

Információbiztonsági helyzetkép - 2012

Rónaszéki Péter, CISA, CISM, ISO27001LA
peter.ronaszeki@isaca.hu